RSA SECURITY

RSA Security Inc.
20 Crosby Drive
Bedford, MA 01730

Tel 781 301 5000
Fax 781 301 5170
www.rsasecurity.com

March 9, 2000

Jim Foti
NIST
100 Bureau Drive, Stop 8930
Building 820, Room 417
Gaithersburg, MD 20899-8930
USA

Dear Jim:

In response to your e-mail message of February 2, 2000 requesting updated patent information for the AES finalists, the patent and patent application information that RSA Security Inc. originally provided to NIST has changed as follows:

1. The patent application "Block Encryption Algorithm with Data-Dependent Rotations" (Serial number 08/854,210) has issued as the following patent:

Title: Block Encryption Algorithm with Data-Dependent Rotations
Patent number: 5,835,600
Date of patent: November 10, 1998
Application number: 845,210
Filed: April 21, 1997
Inventor: Ronald L. Rivest
Assignee: RSA Security Inc.

2. A foreign counterpart of the patent application "Enhanced Block Ciphers with Data Dependent Rotations" (Serial number: 09/094,649) has been filed:

Title: Enhanced Block Ciphers with Data-Dependent Rotations
Serial number: PCT/US99/13358
Filed: June 15, 1999
Inventors: Ronald L. Rivest, M.J.B Robshaw, R. Sidney, Y.L. Yin
Assignee: RSA Security Inc.

(Note that our previous letter gave an incorrect title for the US patent application; the correct title is "Enhanced Block Encryption Algorithm with Data-Dependent Rotations".)

3. The assignee for the various patents and patent applications has been changed to our new corporate name, RSA Security Inc.

RSA Security Inc. affirms that its agreement with NIST's policies regarding AES intellectual property issues includes these new patents and patent applications as well.

Sincerely,

Burton S. Kaliski Jr.
Chief Scientist and Director, RSA Laboratories

cc: Margaret K. Seif, Vice President and General Counsel, RSA Security Inc.